AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Maine

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with selemanikabila@outlook.com that is stored at premises controlled by Microsoft

Case No. 2:16-mj-66-JHR

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A to Affidavit of Special Agent Brendan M. Quinlan, attached

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B to Affidavit of Special Agent Brendan M. Quinlan, attached

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371, 1546(a)	Conspiracy to fraudulently use immigration documents

The application is based on these facts:

Please see the attached Affidavit of Special Agent Brendan M. Quinlan

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Brendan M. Quinlan, DSS
Printed name and title

Sworn to before me and signed in my presence.

Date: 03/07/2016

Judge's signature

City and state: Portland, Maine

John H. Rich III, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT APPLICATION

I, Brendan M. Quinlan, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the account **selemanikabila@outlook.com** ("SUBJECT ACCOUNT") that is stored at premises controlled by Microsoft, an email provider headquartered in Redmond, Washington.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Diplomatic Security Service (DSS), Department of State, and I have been so employed since March 2010. I am currently assigned to the Portsmouth, New Hampshire Resident Office. Over the course of my employment with the State Department, I have investigated a wide variety of matters, including, among other things, immigration crimes, fraud, passport-related crimes and financial crimes. Prior to my employment with the State Department, I was employed as an Immigration Enforcement Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that probable cause exists to believe that a violation of 18 U.S.C. §§ 371 and 1546(a) (conspiracy to fraudulently use immigration documents) has been committed by the user of the SUBJECT ACCOUNT. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. Title 18, United States Code, Section 1546(a) provides that anyone who knowingly uses or attempts to use a document prescribed by statute or regulation for entry into or as evidence of authorized stay in the United States, knowing that it has been unlawfully obtained, commits a crime. Title 18, United States Code, Section 371 provides that anyone who conspires to commit an offense against the United States also commits a crime.

PROBABLE CAUSE

Information Provided by Cooperating Defendant

8. Investigators with DSS and Homeland Security Investigations have been investigating Mukonkole Huge Kifwa and other individuals since approximately March of 2015. On November 17, 2015, a grand jury in the District of Maine returned a superseding indictment which charged Kifwa with one count of visa fraud, two counts of illegal possession of a firearm,

four counts of bank fraud and one count of false statements. On January 14, 2016, a jury in this district found Kifwa guilty of all charges in the indictment.

9. Other investigators and I have continued to investigate Kifwa and his associates for their involvement in other illegal activity. As part of this investigation, on December 11, 2015, and December 18, 2015, I spoke with Eddy Mintela, an associate of Kifwa.[1] Mintela explained that following Kifwa's arrest in July 2015, Mintela was given access to Kifwa's e-mail account by Kifwa and Kifwa's girlfriend, Valerie Mugaruka, in order to obtain documents that Kifwa claimed he needed for his defense against the immigration charges for which he had been arrested. Mintela remembered the address as **selemanikabila@outlook.com**, the SUBJECT ACCOUNT.

10. Mintela told us that after he was given access to the SUBJECT ACCOUNT, he read messages between Kifwa and a person he identified as Mvita Mbambi that were exchanged in the early part of 2015. Mintela identified a known photo of Mbambi. Mintela stated that the messages contained details of an agreement between Mbambi and Kifwa in which Kifwa had paid Mbambi for an effort to smuggle him from the United States into Canada.

---

[1] Mintela, 30, has completed a Plea and Cooperation Agreement with the United States Attorney's Office in Portland, Maine. In this agreement, Mintela has agreed that he has committed Conspiracy to Commit Visa Fraud along with Kifwa and others. Mintela has also admitted to participating in a credit card fraud scheme in which Kifwa also allegedly participated. Although he has agreed to forfeit assets associated with this criminal activity, he has not yet been charged. After being encountered by law enforcement, Mintela was cooperative and all of his information was independently verified. Mintela also testified against Kifwa in his criminal trial, under the terms of his Cooperation Agreement. The information he provided in December 2015 was under the terms of a proffer agreement, under which the government agreed not to make direct use of Mintela's statements in the proffer.

11. Mintela told us that in the emails, Kifwa and Mbambi discussed the fact that although Kifwa had paid Mbambi, the effort to smuggle him from the United States into Canada had not been successful.

Kifwa's Recorded Telephone Conversation

12. During his pre-trial incarceration at the Cumberland County Jail, on October 25, 2015, Kifwa was recorded on the inmate telephone speaking to an associate about unnamed individuals, "two guy and two lady," all who knew each other in Africa, who were making "fake invitation" and "fake organization" to get people to come to the United States from South Africa, Congo, and Angola, and then subsequently getting them into Canada. Kifwa also stated that some of these unnamed individuals owed him money.

13. I have listened to this conversation. Based on my experience in this investigation, it is my belief that Mbambi is one of the unnamed individuals Kifwa discussed in the recorded conversation.

Related Activity by Mbambi

14. On April 12, 2014, Mvita Mbambi was arrested by the Canada Border Services Agency (CBSA) at the Woodstock, New Brunswick Port of Entry into Canada (directly across the border from Houlton, Maine) for violations of section 131 of the Immigration and Refugee Protection Act: Attempting to aid or abet persons using fraudulently obtained U.S. identity documents in order to gain entry to Canada. I have read the CBSA report of this event. Mbambi was driving across the US-Canada international border in a car that was also occupied by two other persons, one from the Democratic Republic of the Congo, the other from Angola. Both were found to be in possession of U.S. travel documents that were not their own: one had a valid U.S. passport that belonged to someone else, and the other had a valid permanent resident card

that belonged to someone else. CBSA has informed DSS and HSI that Mbambi fled Canada after his arrest and there is an active warrant for his arrest.

15. I have also reviewed CBSA records regarding prior entries into Canada by Mbambi. These records show that on seven occasions between March 2013 and April 2014, Mbami entered Canada in the company of an individual holding United States passport number xxxxx6666, issued to A.M. On each occasion, Mbambi re-entered the United States alone. I have also reviewed Department of Homeland Security records showing no entries into the United States from Canada by A.M from January 1, 2014, to the present. Based on my experience in this investigation and my training and experience in other investigations, I believe this information shows that Mbambi has been bringing multiple people into Canada from the United States using A.M.'s passport.

Additional Investigation

16. I have reviewed records kept by the U.S. Department of State and U.S. Department of Homeland Security that show Mbambi was born in the Democratic Republic of Congo but subsequently became a naturalized United States Citizen on November 19, 1996, and currently holds a U.S. passport.

17. Both Kifwa and Mbami currently live in Maine, and both lived in Maine at the time of the emails recounted by Mintela. Mbambi listed 40 Anderson Street in Portland as his permanent address on a U.S. Department of State form as early as August 26, 2014. His latest Maine driver's license lists the same address and was issued on May 18, 2012. I went to this residence on November 9, 2015, and although he was not home, a woman who identified herself as Abusana Bondo, Mbambi's wife, stated he lived there. Evidence from bank accounts and

testimony from witnesses have shown that Kifwa has been living in the Portland, Maine area since at least November 2014.

18. On February 2, 2016, I spoke with a representative of Bank of America, who told me that the SUBJECT ACCOUNT was used by "Adrien Lushiku" to open an account in Texas in 2014. Adrien Lushiku is a known alias of Munkonkole Huge Kifwa.

19. On December 11, 2015, pursuant to 18 U.S.C. § 2703(f), I sent a preservation letter to Microsoft for the SUBJECT ACCOUNT, requesting the preservation of all information associated with the account, including email content.

20. Based on the above facts, I submit that probable cause exists to believe that Kifwa and Mbambi communicated using the SUBJECT ACCOUNT in furtherance of a conspiracy to fraudulently use immigration documents, in violation of 18 U.S.C. §§ 371 and 1546(a). Accordingly, I submit that probable cause exists to believe that evidence of this illegal conduct will be found in the SUBJECT ACCOUNT.

BACKGROUND CONCERNING EMAIL

21. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including email access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name outlook.com, such as **selemanikabila@outlook.com**. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of the provider is likely to contain stored electronic communications (including retrieved and un-retrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. In my training and experience, in general, an email that is sent to a Microsoft email subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

23. In my training and experience, Microsoft subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the provider. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

24. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location or illicit activities.

25. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

26. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled

the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

28. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft, which will then compile the requested records at a time convenient to it, I submit that reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Dated this 7th day of March, 2016

Respectfully submitted,

Brendan M. Quinlan
Special Agent
Department of State

Subscribed and sworn to before me on March 7, 2016

John H. Rich III
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **selemanikabila@outlook.com** that is stored at stored at premises controlled by Microsoft, an email provider headquartered in Redmond, Washington.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on December 11, 2015, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 371 and 1546(a) (conspiracy to fraudulently use immigration documents), this violation occurring after January 1, 2015, including, for the account listed on Attachment A, information pertaining to the following matters:

a. Any and all electronic correspondence containing discussions about or references to travel to Canada or elsewhere under fraudulent pretenses; the unlawful use of U.S. travel documents; obtaining visas to facilitate the immigration of foreign nationals to the United States; and/or the payments in money, goods or services for such crimes.

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

e. The identity of the person(s) who communicated with the user ID about matters relating to visas, immigration and or/payments including records that help reveal their whereabouts; and

f. Evidence of any financial gain or profits associated with the aforementioned alleged criminal activity.